



## INFORMATION SECURITY INCORPORATED

1001 Spring Street, Suite 123  
Silver Spring, Maryland 20910

(301) 565-8168  
FAX (301) 565-8167



February 13, 1997

Nancy Crowe  
Regulatory Policy Division  
Bureau of Export Administration  
Department of Commerce  
14th and Pennsylvania Ave., N.W., Room 2705  
Washington, D.C. 20230

BY FAX AND MAIL

**Subject: Comment on Interim Rule for Encryption Items, 61FR68572-68587**

Dear Ms Crowe:

1. The interim rule summary states that this rule is intended to make it easier for Americans to use stronger encryption products to protect their privacy, intellectual property and other valuable information. Nowhere in the actual regulations, including the policy sections, is there a reaffirmation or encouragement to U.S. persons (individuals, companies, organizations, etc.) that the previous U.S. Government policy of approving exports of cryptography for the purpose of protecting U.S. business data and interests will be continued. As you know U.S. firms and individuals, as a rule, received Department of State export licenses for themselves and affiliates and agents for commodities such as non-key escrow or non-key recovery 56 bit DES encryption to protect their information outside the United States and Canada.

**Recommendation:** The interim rule should be amended to emphasize that as a general rule, export licenses will be approved for encryption items such as standard (i.e. non-key escrow and non-key recovery) 56 bit key DES (and/or perhaps other algorithms and key lengths) for the purpose of protecting U.S. business and personal information from exploitation.

2. The stated concept of a "worldwide key management infrastructure with the use of key escrow and key recovery encryption items" seems contradictory, expensive, and a threat to U.S. private sector and government interests.

a) Which non-U.S. organizations or people would operate such an infrastructure? Public statements from the FBI, CIA, and other organizations identify a wide range of traditional military allies as well as traditional adversaries that actively conduct or sponsor economic espionage activities against U.S. businesses, persons and government. I believe, if both the unclassified and classified data were searched, one would be hard pressed to name a single country that we could trust to operate a key recovery center which would allow for the decryption of U.S. business, personal, or

Nancy Crowe  
February 13, 1997  
Page 2

government cryptographically protected information when that information would provide an advantage to that foreign country or to its businesses.

b) Operating a 24 hour "key recovery management center" is an extremely complex and expensive operation and only elements of the U.S. Government have real world experience in key management on this scale. If U.S. business is expected to make a rational economic decision as to whether or not they will offer "key recovery" cryptography in exchange for liberalization of export approval, the U.S. Government should provide estimates as to what it would cost to develop and operate such a center.

c) The requirements for a key recovery agent are woefully inadequate. A secret clearance and/or a favorable credit check, criminal records check, and performance bond check could met by the simple procedure of creating a false identity. A minimum of a Top Secret clearance with full background investigation or equivalent seems much more appropriate.

d) It was stated in public testimony that Mr. Whitworth of the Walker spy ring acted as a "key recovery" agent for the Soviets allowing them to read over one million classified messages. This demonstrates how difficult it is to securely manage cryptographic keys *without the built in vulnerability of key escrow and recovery.*

**Recommendation:** Seriously reconsider the entire concept of key escrow and worldwide key recovery.

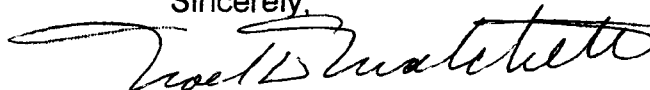
**Recommendation:** Provide the public justified cost estimates for operating a key recovery center.

**Recommendation:** Upgrade the requirements for a key recovery agent to Top Secret clearance with full background or equivalent.

**Recommendation:** Concentrate scarce resources on meeting the information security requirements of U.S. business, individuals, and government.

**Recommendation:** All key recovery operations should be under and only under the direct control of approved and reliable U.S. citizens. Under no circumstances should any encryption key to U.S. encrypted traffic be shared with a non U.S. person, government, or organization except those involving obvious terrorist, espionage, and international criminal activities.

Sincerely,



Noel D. Matchett  
President